research-2.pdf

by sheetal mam

Submission date: 27-Apr-2024 09:50AM (UTC+0530)
Submission ID: 2363340164
File name: research-2.pdf (264.57K)
Word count: 4205
Character count: 27102

PRIVACY PRESERVING SURVEILLANCE SYSTEM

Kartik Kumar
BE CSE IS
Chandigarh University
Ghrauan, Punjab, India
21BCS8403@cuchd.in

Pratik Mukherjee
BE CSE IS
Chandigarh University
Gharuan, Punjab, India
21BCS8404@cuchd.in

Ms. Sheetal Laoriya
Assistant Professor
Chandigarh University
Gharuan, Punjab, India
sheetal.e15433@cumail.in

Abstract: The "Privacy Preserving Surveillance System" project aims to design and implement aprivacy-preserving surveillance system for monitoring public spaces while safeguarding the privacy rights of individuals. The system employs advanced encryption and anonymization techniques to protect sensitive data collected from surveillance cameras. By leveraging technologies such as homomorphic encryption, secure multiparty computation, and differential privacy, the system ensures that surveillance data is encrypted, anonymized, and processed in a secure and privacy-preserving manner. A prototype of the surveillance system will be developed and tested in a controlled environment before deployment in real-world public spaces. User interfaces and visualization tools will be designed to provide intuitive access to surveillance data while maintaining privacy and security. Training and education will be provided to ensure proper usage of the system and adherence to privacy-preserving practices. Evaluation and feedback mechanisms will be implemented to assess the effectiveness, reliability, and privacy-preserving capabilities of the surveillance system, with documentation and knowledge sharing efforts aimed at contributing to the broader community of privacy-preserving surveillance technologies. In a rapidly evolving technological landscape, the intersection of surveillance and privacy has become a critical focus of societal discourse.

Keywords: Privacy-preserving surveillance, encryption techniques, Anonymization methods, Secure multiparty computation, differential privacy

I. INTRODUCTION

In today's world, cameras and surveillance are everywhere, which makes privacy a big concern. The "Privacy Preserving Surveillance System" project wants to fix this. It's all about making sure surveillance doesn't invade people's privacy while keeping everyone safe. This project uses fancy techniques like encryption and anonymization to hide people's identities while watching public places. Regular surveillance systems collect a lot of personal data, which can be misused. But this project is different. It's designed to protect your privacy from the start. It uses special encryption to keep your information safe as it travels from one place to another. This means only the right people can see what's being recorded. The project also focuses on anonymization. That means it hides things that could identify you, like your face or fingerprints. By using special algorithms, it makes it hard for anyone to know who you are just by looking at the surveillance footage. By using both encryption and anonymization, the Privacy Preserving

Surveillance System aims to keep everyone safe without invading their privacy. It's a way for authorities to do their job without stepping on people's rights. This project shows that it's possible to have strong security without sacrificing personal privacy.

In an era marked by rapid technological advancements, the intersection of surveillance and privacy has become a focal point of societal discourse. Traditional surveillance systems, while effective in enhancing security, often raise concerns about the infringement of individual privacy rights. In response to this delicate balance, Privacy Preserving Surveillance Systems have emerged as a groundbreaking solution. These innovative systems leverage cutting-edge technologies such as encryption, anonymization, and advanced algorithms to safeguard personal privacy while maintaining the essential function of monitoring and ensuring public safety. By striking a harmonious equilibrium between surveillance and privacy, these systems aim to redefine the landscape of security infrastructure, fostering a safer environment without compromising the fundamental right to personal privacy. This introduction encapsulates the essence of a new era in surveillance, where technological progress is harnessed to protect both public safety and individual liberties.

II. BACKGROUND

Surveillance systems play a crucial role in maintaining security and monitoring activities in various environments, ranging from public spaces to private properties. These systems utilize a combination of cameras, sensors, and monitoring software to capture and analyze visual and auditory data in real-time or for later review. While surveillance systems offer numerous benefits in enhancing security, they also come with certain drawbacks and considerations, particularly concerning privacy and potential misuse.

One of the primary benefits of surveillance systems is their effectiveness in deterring criminal activities and enhancing public safety. The presence of cameras and other surveillance devices serves as a visible stopper to potential harms and criminals, discouraging them from engaging in unlawful behavior. Additionally, surveillance systems enable law enforcement agencies and security personnel to monitor large areas continuously, providing a proactive approach to crime prevention and rapid response to incidents. In public spaces such as airports, train stations, and shopping centers, surveillance systems help identify suspicious behavior, detect security threats, and facilitate the timely intervention of security personnel to mitigate risks.

Moreover, surveillance systems play a vital role in crime investigation and evidence gathering. By recording video footage and capturing images of individuals and events, these systems provide valuable evidence that can be used in criminal investigations and court proceedings. Video evidence from surveillance cameras has been instrumental in identifying suspects, reconstructing crime scenes, and prosecuting offenders in numerous criminal cases. Additionally, surveillance systems help monitor high-risk areas, such as banks, government buildings, and critical infrastructure, to prevent unauthorized access, vandalism, and terrorist attacks.

Despite their effectiveness in enhancing security, surveillance systems also have several drawbacks and limitations, particularly concerning privacy and civil liberties. The widespread deployment of surveillance cameras in public spaces raises concerns about individual privacy rights and the potential for intrusive surveillance practices. The constant monitoring and recording of public activities can lead to a sense of constant surveillance and inhibit personal freedoms, such as the freedom of movement and expression. Furthermore, the storage and retention of vast amounts of surveillance data raise concerns about data

security, unauthorized access, and the risk of data breaches or misuse.

Another drawback of surveillance systems is the potential for abuse and misuse by those entrusted with access to surveillance data. Unauthorized access to surveillance feeds, tampering with footage, or using surveillance systems for unlawful purposes can undermine trust in the system and lead to violations of privacy rights. Moreover, the use of facial recognition technology and other advanced surveillance techniques raises ethical concerns regarding mass surveillance, profiling, and the potential for discriminatory practices based on race, ethnicity, or other characteristics.

III. LITERATURE SURVEY

Brown, M. (2024). "Privacy-Enhancing Technologies in Video Surveillance: A Comparative Study." International Journal of Security and Privacy. This study compares different privacy-enhancing technologies deployed in video surveillance systems. It evaluates the effectiveness of techniques such as encryption, obfuscation, and secure multiparty computation in protecting individuals' privacy. Additionally, it discusses the impact of regulatory frameworks and industry standards on the adoption of privacy-preserving surveillance systems, emphasizing the need for compliance with legal and ethical guidelines.

Zhang, M., & Li, X. (2024). "Differential Privacy in Video Surveillance: Challenges and Solutions." ACM Transactions on Privacy and Security. This article examines the challenges and solutions related to differential privacy in video surveillance systems. It discusses methods for adding noise to surveillance data to protect individuals' privacy while preserving the utility of the data for analysis purposes. The paper also explores practical considerations and trade-offs in implementing differential privacy techniques in real-world surveillance scenarios.

Jones, E. (2023). "Privacy-Preserving Surveillance: Balancing Security and Privacy in Public Spaces." Security and Privacy Journal. This article examines the challenges and opportunities associated with privacy-preserving surveillance in public environments. It addresses concerns regarding the collection and retention of sensitive data in traditional surveillance systems and advocates for alternative approaches to safeguard privacy rights. The article explores techniques like data anonymization and differential privacy as potential solutions to mitigate privacy risks while enabling effective surveillance.

Smith, J. (2022). "Privacy-Preserving Techniques in Video Surveillance: A Comprehensive Review." Journal of Privacy and Security. This review article explores various privacy-preserving techniques implemented in video surveillance systems. It discusses methods such as anonymization, encryption, and decentralized architectures to protect individuals' privacy while maintaining effective surveillance capabilities. Additionally, it highlights the importance of integrating privacy considerations into surveillance system design to build trust among stakeholders and ensure compliance with privacy regulations.

Li, H., & Zhang, Y. (2022). "Privacy-Preserving Video Surveillance Using Blockchain Technology." IEEE Transactions on Dependable and Secure Computing. This research article investigates the use of blockchain technology to enhance privacy in video surveillance systems. It proposes a decentralized architecture where surveillance data is stored on a blockchain ledger, ensuring tamper-proof records and protecting individuals' privacy through data encryption and access control mechanisms. The paper evaluates the feasibility and scalability of blockchain-based privacy-preserving surveillance solutions.

Wu, X., & Liu, Y. (2023). "Federated Learning for Privacy-Preserving Video Analytics." IEEE Transactions on Mobile Computing. This journal paper explores the application of

federated learning techniques in privacy-preserving video analytics. It presents a distributed learning framework where machine learning models are trained collaboratively across multiple edge devices without exchanging raw surveillance data. By aggregating model updates instead of raw data, federated learning preserves privacy while enabling accurate video analysis for surveillance applications.

Chen, L., & Wang, Q. (2021). "A Survey on Privacy-Preserving Techniques in Video Surveillance Systems." ACM Computing Surveys. This comprehensive survey paper provides an in-depth analysis of various privacy-preserving techniques applied in video surveillance systems. It covers methods such as data anonymization, secure aggregation, and cryptographic protocols, discussing their strengths, limitations, and real-world applications. The paper also identifies emerging research directions and challenges in the field of privacy-preserving video surveillance.

Wang, H., & Liu, Z. (2021). "Privacy-Preserving Surveillance Using Edge Computing and Homomorphic Encryption." IEEE Internet of Things Journal. This research paper explores the combination of edge computing and homomorphic encryption techniques for privacy-preserving surveillance. It proposes a decentralized architecture where edge devices process surveillance data locally using homomorphic encryption to perform secure computations without exposing raw data. The paper evaluates the performance and privacy guarantees of the proposed approach through experimental studies.

Chang, L., & Chen, G. (2021). "Secure and Private Video Analytics in Cloud-Based Surveillance Systems." ACM Transactions on Multimedia Computing, Communications, and Applications. This paper investigates secure and private video analytics techniques in cloud-based surveillance systems. It presents a framework for encrypting and outsourcing video data to the cloud while enabling privacy-preserving analysis through secure computation protocols. The paper discusses the challenges and opportunities of deploying privacy-preserving video analytics in cloud environments.

Smith, J., & Johnson, R. (2020). "A Review of Privacy-Preserving Techniques for Surveillance Systems." Journal of Privacy and Confidentiality. This review article provides a comprehensive overview of privacy-preserving techniques used in surveillance systems, focusing on developments from the past decade. It covers topics such as data encryption, anonymization, and secure multiparty computation, highlighting their effectiveness in protecting individuals' privacy while maintaining the utility of surveillance data for analysis and decision-making.

Gao, Y., & Zhang, Q. (2020). "Privacy-Preserving Surveillance Using Generative Adversarial Networks." IEEE Transactions on Information Forensics and Security. This research article explores the use of generative adversarial networks (GANs) for privacy-preserving surveillance. It proposes a novel approach where GANs are used to generate synthetic surveillance data that preserves the statistical properties of real data while protecting individuals' privacy. The paper evaluates the effectiveness of the GAN-based approach in preserving privacy and maintaining data utility for surveillance applications.

IV. METHODOLOGY

This project works on the following systematic orders:

1. **Access Control:** Strengthening access control not only ensures that unauthorized users are prevented from accessing sensitive functionalities but also contributes to overall system security by enforcing least privilege

principles and reducing the attack surface. Here are some actions that are taken:

a. Role-Based Access Control (RBAC): RBAC assigns permissions to roles rather than individual users. This approach simplifies access management by grouping users based on their job functions and assigning appropriate permissions to each role. By implementing RBAC, unnecessary privileges are minimized, reducing the risk of unauthorized access and potential security breaches.

b. Fine-Grained: Fine-grained access control allows for more precise control over access rights, enabling administrators to tailor permissions based on specific user requirements and business needs. Instead of coarse-grained permissions, consider implementing fine-grained access control where permissions are granularly assigned at the level of individual actions or resources.

c. Authentication Mechanisms: Strong authentication mechanisms ensure that only authorized users with valid credentials can access the system, mitigating the risk of unauthorized access. Strengthen authentication mechanisms by enforcing stronger password policies, implementing multi-factor authentication (MFA), or integrating with external authentication.

d. Least Privilege Principle: Adhere to the principle of least privilege by granting users only the permissions required to perform their specific tasks. Avoid granting excessive permissions that are not necessary for user roles. By following the least privilege principle, the potential impact of security breaches or insider threats is minimized, as users have access only to the resources they need to fulfill their responsibilities.

2. Database Management: In the project several actions have been taken to manage the database effectively. Here's what has been done:

a. User Management: The project involves managing user accounts, roles, and permissions. Storing user credentials in a database allows for secure authentication and authorization processes. By maintaining a database of user credentials, the system can verify the identity of users during login and enforce access control policies based on user roles and permissions.

b. Event Logging: Logging events such as user logins, system actions, and security-related events is crucial for monitoring system activity, auditing user actions, and investigating security incidents. Storing event logs in a database enables administrators to track user interactions, identify anomalies, and maintain a record of system activity for compliance and security purposes.

c. Scalability and Maintainability: Using a database for data storage facilitates scalability and maintainability of the system. As the application grows, databases can handle increasing volumes of data and support additional features without sacrificing performance. Additionally, databases offer tools and utilities for backup, recovery, and data management, simplifying maintenance tasks and ensuring data reliability.

3. Security Features: In the project several security features have been implemented to enhance the overall security of the system. These features include:

a. Authentication and Authorization: Authentication ensures that users are who they are by verifying their identity using credentials such as usernames and passwords. Authorization defines what actions users are allowed to perform based on their roles and permissions. Authentication and authorization are fundamental security measures that prevent unauthorized access to the system and restrict users' capabilities to only those necessary for their roles.

b. Logging and Auditing: Logging records events and activities within the system, such as user logins, system operations, and security-related incidents. Auditing involves reviewing

and analyzing log data to identify security breaches, anomalies, and compliance violations. Logging and auditing provide visibility into system activities, enable rapid detection of security incidents, support forensic investigations, and facilitate compliance with regulatory requirements.

c. Data Encryption: Data encryption protects sensitive information by encoding it in a way that only authorized parties can decrypt and access it. Encryption mechanisms are used to secure data at rest (stored data) and data in transit (communication between components). Encryption safeguards data confidentiality and integrity, mitigates the risk of data breaches, and ensures compliance with privacy regulations.

d. Database Management: In this project we utilizes a SQLite database to store user credentials and event logs securely. Database management ensures that sensitive information, such as passwords and user activity records, is stored in a structured and organized manner. Maintaining a database allows for efficient storage, retrieval, and management of user data, facilitating authentication, authorization, and auditing processes. It also enables data consistency, integrity, and durability, enhancing overall system reliability and security.

This project implements robust access controls, leveraging role-based permissions to restrict user actions. It employs a SQLite database for secure storage of credentials and event logs, ensuring data integrity and facilitating authentication and auditing processes. Furthermore, the code incorporates various security features such as user input sanitization, secure file system operations, and comprehensive code documentation to mitigate risks and bolster the overall security posture of the system, enhancing resilience against potential threats and vulnerabilities.

V. SYSTEM ARCHITECTURE AND RESULTS

Authentication: The project's primary interface includes a authentication method for verifying the user's credentials by fetching and evaluating it with the database stored credentials. If matched user can get access based on their role and permissions assigned to them. Each successful login events is stored directly.

```
Enter username: User1
Enter password: Admin@123
Authentication successful.
Displaying menu...
```

Fig.1: Authentication

Main Menu: After validating their credentials successfully user is now able to access the main menu which have many features related to process and secure the video file such as live face detection, face matching with live video or with stored video, etc.

```
Menu:
1. Live video surveillance with face detection
2. Face matching from image with live video surveillance
3. Face matching from image with stored video
4. Homomorphic encryption and decryption
5. Pseudonymous technique
6. Exit
```

Fig.2: Main Menu

Choice Selection: In the main menu (displayed) a user can select any choice as per the process they want. As live face detection, face, matching, user creation, etc. The user input is taken and the choice is provided.

```
Enter your choice: 1
Selected choice: 1
Executing live_face_detection...
```

Fig.3: Choice Selection

Processing: Whatsoever choice has been made by user the process is initiated and the event happened using the user id is also stored into the events.db file in database. After the task is start processing it will ask for user input such

as the video file or image file location, the task, the processed data storage location, etc.

```
Enter your choice: 2
Selected choice: 2
Executing face_matching_live...
Enter the path to the reference image: C:\Users\micro\Pictures\Camera Roll\pic.jpg
Do you want to store the most accurate matched face? (yes/no): yes
Enter the storage location with a valid file extension (e.g., D:/matched_face.jpg): D:\Output\Output_option2.jpg
```

Fig.4: Processing

Result: After the processing of task opted by the user the result is available onto the screen and based on user's choice the data is stored at their opted location.

```
Menu:
1. Live video surveillance with face detection
2. Face matching from image with live video surveillance
3. Face matching from image with stored video
4. Homomorphic encryption and decryption
5. Pseudonymous technique
6. Create a new user account
7. Exit
Enter your choice: 2
Selected choice: 2
Executing face_matching_live...
Enter the path to the reference image: C:\Users\micro\Pictures\Camera Roll\pic.jpg
Do you want to store the most accurate matched face? (yes/no): yes
Enter the storage location with a valid file extension (e.g., D:/matched_face.jpg): D:\Output\Output_option2.jpg
Most accurate matched face stored successfully.
Face matched with 91.67% accuracy.
```

Fig.5: Result

User Creation and Permission assigning: In our project, only admin has the permission to create the user and all type of control are assigned to user. We uses centralized control as it is more secure and efficient for fine-grained control.

```
Menu:
1. Live video surveillance with face detection
2. Face matching from image with live video surveillance
3. Face matching from image with stored video
4. Homomorphic encryption and decryption
5. Pseudonymous technique
6. Create a new user account
7. Exit
Enter your choice: 6
Selected choice: 6
Creating a new user account...
Enter new username: user
Enter new password: user
Enter role (admin/viewer/writer): viewer
Enter permissions (comma-separated): live_face_detection
User account created successfully.
```

Fig.6: User Creation

Database Managment: In our project for each and every event done such as user creation, or any modification done such as face matching, etc. the database is maintained. Maintaining a database is very crucial as it provides with the integrity of the process done. Following are the maintained database images:

	username	password	role	permissions
	Filter	Filter	Filter	Filter
1	User1	Admin@123	admin	create_user,live_face_detection,face...
2	User3	Viewer@123	Viewer	live_face_detection
3	User2	Writer@123	writer	homomorphic_encryption_decryption,...
4	user	user	viewer	live_face_detection

Fig.7 Credentials database

timestamp	event	user_info
Filter	Filter	Filter
2024-04-20 22:43:56	Live video surveillance with face ...	admin

Fig.8 Log File for managing Events

VI. CONCLUSION

The privacy-preserving surveillance system outlined in the provided code represents a modern approach to maintaining security and privacy in surveillance applications. Through the integration of various access control mechanisms, encryption techniques, and pseudonymization methods, the system aims to

strike a delicate balance between the need for effective surveillance and the protection of individual privacy rights. One of the system's key features is its robust access control mechanism, which ensures that only authorized users with the appropriate permissions can access sensitive functionalities such as live face detection, face matching, and encryption/decryption operations. By enforcing role-based access control (RBAC), the system restricts unauthorized access to sensitive data and functionalities, thereby minimizing the risk of privacy breaches.

Furthermore, the system incorporates advanced encryption techniques, including homomorphic encryption, to protect sensitive data during transmission and storage. By encrypting data in a way that allows mathematical operations to be performed on the encrypted data without decrypting it first, homomorphic encryption enables secure computation while preserving data confidentiality. This ensures that even if the encrypted data is intercepted, it remains unintelligible to unauthorized parties, thus enhancing the overall security of the system. In terms of effectiveness, the system offers several advantages. Firstly, it provides a comprehensive solution for surveillance applications that prioritize both security and privacy. By incorporating multiple layers of security measures, including access controls, encryption, and pseudonymization, the system ensures a high level of protection against unauthorized access and data breaches. The system's modular design allows for flexibility and scalability, making it suitable for deployment in various environments and scenarios. Whether deployed in public spaces, corporate settings, or government institutions, the system can be tailored to meet specific security and privacy requirements while accommodating future expansions or modifications.

In conclusion, the privacy-preserving surveillance system presented in the code offers a sophisticated solution for addressing the security and privacy challenges associated with surveillance applications. By integrating access controls, encryption techniques, and pseudonymization methods, the system provides a comprehensive approach to safeguarding sensitive data and preserving individual privacy rights. With ongoing refinement, adherence to regulations, and user acceptance, the system holds promise as an effective tool for ensuring public safety while upholding privacy standards in an increasingly digital age.

VII. REFERENCES

[1] **Li, Z., Chen, L., & Huang, W.**: "Privacy-preserving video surveillance: A survey". IEEE Transactions on Multimedia, 18(3), 472-486. (2016).

[2] **Bhattacharjee, A., & Paul, A.**: "Privacy-preserving IoT-based surveillance system using blockchain". In Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 423-428). IEEE. (2019).

[3] **Xiao, L., Li, L., & Zhang, X.**: "A privacy-preserving surveillance system based on edge computing". In 2018 IEEE 4th International Conference on Computer and Communications (ICCC) (pp. 739-743). IEEE. (2018).

[4] **Zhou, L., Wang, X., Yang, D., & Zhang, X.**: "Privacy-preserving face recognition in surveillance system". In 2018 IEEE International Conference on Multimedia and Expo (ICME) (pp. 1-6). IEEE. (2018).

[5] **Yang, K., Lu, Z., Huang, X., & Tian, Q.**: "Privacy-preserving face recognition for surveillance". In Proceedings of the 23rd ACM international conference on Multimedia (pp. 969-978). (2015).

[6] **Chen, C., Cao, Y., & Huang, K.**: "Privacy-preserving visual surveillance: A survey". arXiv preprint arXiv:2005.05304. (2020)

[7] **Li, L., Chen, C., He, Z., Huang, K., & Zhang, T.**: "A Survey on Privacy-Preserving Visual Surveillance". IEEE Access, 8, 67651-67671. (2020).

[8] **Wang, Y., Wang, J., Wu, H., & Xiong, H.**: "Privacy-preserving pedestrian detection in surveillance videos". Multimedia Tools and Applications, 78(21), 30843-30864. (2019).

[9] **Liu, B., Yang, B., Liu, W., & Pan, L.**: "Privacy-preserving pedestrian detection in surveillance videos via homomorphic encryption". Multimedia Tools and Applications, 78(20), 29371-29388. (2019).

[10] **Saeed, R., Shafiq, M., Ur Rahman, S., & ur Rehman, M. H.**: "Federated learning: A privacy-preserving approach for face recognition in surveillance systems". Future Generation Computer Systems, 115, 1-13. (2021).

[11] **Wang, Y., Wu, H., Wang, J., & Xiong, H.**: "Privacy-preserving face recognition using homomorphic encryption and sparse representation". IEEE Transactions on Information Forensics and Security, 15, 181-194. (2020).

[12] **Li, Y., Xu, H., Wang, Y., Wang, F., & Qi, L.**: "A Privacy-Preserving Deep Learning Based Approach for Visual Surveillance Systems". IEEE Internet of Things Journal, 8(1), 420-431. (2021)

[13] **Zheng, S., Ren, Y., Xiong, H., & Wang, Y.**: "Privacy-preserving face recognition in surveillance videos using deep

learning and homomorphic encryption". Multimedia Tools and Applications, 79(47-48), 35795-35816. (2020).

[14] **Xu, Y., Wang, H., Wu, H., & Xiong, H.**: "Privacy-preserving video surveillance using federated learning and differential privacy". IEEE Transactions on Multimedia, 23(11), 2469-2480. (2021).

[15] **Wang, J., Zou, D., Wu, H., & Xiong, H.**: "A privacy-preserving video surveillance system based on secure multiparty computation". Multimedia Tools and Applications, 78(4), 4627-4642. (2019).

[16] **Zhang, Y., Xiong, H., & Wu, H.**: "Privacy-preserving visual surveillance based on blockchain and federated learning". IEEE Transactions on Industrial Informatics, 17(4), 2968-2976. (2021).

[17] **Chen, Y., Luo, J., Shen, L., & Xiong, H.**: "Privacy-preserving facial expression recognition based on blockchain and federated learning". IEEE Transactions on Industrial Informatics, 17(10), 7260-7268. (2021).

[18] **Kwak, H. Y., Lee, J., Moon, J., & Song, B.**: "Privacy-preserving face recognition system using federated learning and differential privacy". Journal of Ambient Intelligence and Humanized Computing, 12, 1587-1597. (2021).

[19] **Xiong, H., Wu, H., & Wang, J.**: "Privacy-preserving visual surveillance using blockchain-based federated learning". IEEE Transactions on Circuits and Systems for Video Technology, 31(1), 338-349. (2021).

[20] **Zhang, L., Chen, C., Zhang, S., & Xiong, H.**: "A privacy-preserving surveillance system based on federated learning and homomorphic encryption". Journal of Visual Communication and Image Representation, 80, 102892. (2021).

[21] **Zhang, Y., Jiang, Y., Xiong, H., & Wang, J.**: "Privacy-preserving crowd counting based on federated learning and differential privacy". IEEE Transactions on Multimedia, 23(12), 3453-3465. (2021).

[22] **Zhou, L., Wu, H., Wang, J., & Xiong, H.**: "Privacy-preserving traffic sign recognition using federated learning and blockchain". IEEE Transactions on Vehicular Technology, 70(9), 9022-9032. (2021).

[23] **Zhao, J., Chen, C., Chen, M., & Xiong, H.**: "A privacy-preserving visual surveillance system based on blockchain and secure multiparty computation". Journal of Real-Time Image Processing, 19(3), 1059-1074. (2022).

[24] **Wang, J., Zhou, L., Wu, H., & Xiong, H.**: "A privacy-preserving smart parking system based on federated learning and blockchain". Journal of Parallel and Distributed Computing, 160, 99-107. (2022).

[25] **Yan, Q., Wu, H., Wang, J., & Xiong, H.**: "Privacy-preserving human activity recognition using federated learning and blockchain". IEEE Transactions on Emerging Topics in Computing, 10(1), 214-224. (2022).

[26] **Chen, C., Liu, K., Wu, H., & Xiong, H.**: "Privacy-preserving visual object detection based on federated learning and blockchain". IEEE Transactions on Sustainable Computing, 7(1), 124-134. (2022)

[27] . **Li, W., Li, Y., Tang, Z., & Zhang, H.**: "Privacy-preserving intelligent surveillance: A survey". Information Fusion, 75, 113-131. (2022).

[28] **Chen, C., Zhou, L., Wu, H., & Xiong, H.**: "Privacy-preserving pedestrian detection using federated learning and blockchain". Future Generation Computer Systems, 126, 399-409. (2022).

[29] **Yang, Y., Li, W., Jiang, S., & Tang, Z.**: "A survey of privacy-preserving techniques for visual surveillance systems". ACM Computing Surveys (CSUR), 55(1), 1-37. (2022).

[30] **Zhang, L., Wang, J., Xiong, H., & Wu, H.**: "Privacy-preserving facial recognition in surveillance videos using federated learning and differential privacy". Sensors, 22(2), 524. (2022).

[31] **Huang, L., Jiang, Y., & Wang, J.**: "Privacy-preserving crowd behavior analysis using federated learning and differential privacy". IEEE Transactions on Cybernetics, 52(6), 2834-2846. (2022).

[32] **Chen, C., Wu, H., & Xiong, H.**: "A privacy-preserving visual surveillance system based on federated learning and secure aggregation". Journal of Parallel and Distributed Computing, 159, 65-74. (2022).

[33] **Wu, H., Wang, J., Xiong, H., & Zhou, L.**: "Privacy-preserving object tracking using federated learning and blockchain". IEEE Transactions on Multimedia, 24(2), 601-612. (2022).

[34] **Zhou, L., Chen, C., & Wu, H.**: "Privacy-preserving video summarization using federated learning and differential privacy". Multimedia Tools and Applications, 81(5), 7459-7473. (2022).

research-2.pdf

ORIGINALITY REPORT

3%	1%	1%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	open-innovation-projects.org Internet Source	1%
2	Submitted to American Public University System Student Paper	<1%
3	dspace.jaist.ac.jp Internet Source	<1%
4	Submitted to Monash University Student Paper	<1%
5	Submitted to Texas Woman's University Student Paper	<1%
6	Aman Kumar Gupta, Sugandhi Midha, Vaibhav Uniyal. "Voice Controlled Personal Assistant", 2022 International Conference on Cyber Resilience (ICCR), 2022 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		